

A theorem of complete reducibility for exponential polynomials

P. D'Aquino* and G. Terzo†

June 29, 2012

Abstract

In this paper we give a factorization theorem for the ring of exponential polynomials in many variables over an algebraically closed field of characteristic 0 with an exponentiation. This is a generalization of the factorization theorem due to Ritt in [7].

1 Introduction

Ritt in [7] was the first to consider a factorization theory for exponential polynomials over the complex field of the form

$$f(z) = a_1 e^{\alpha_1 z} + \dots + a_n e^{\alpha_n z}, \quad (1)$$

where $a_i, \alpha_i \in \mathbb{C}$. Contributions by Gourin and Macoll in [5] and [6] gave refinements of Ritt's result for exponential polynomials of the form

$$f(z) = p_1(z) e^{\alpha_1 z} + \dots + p_n(z) e^{\alpha_n z}, \quad (2)$$

where α_i are complex numbers and $p_i(z) \in \mathbb{C}[z]$. Only in the mid 1990's van der Poorten and Everest obtained a factorization theorem which applies to exponential polynomials of the form (2) over any algebraically closed field of characteristic 0. In [4] they state (without proving) that their result applies to a more general setting

*Department of Mathematics, Seconda Università di Napoli, Via Vivaldi 43, 81100 Caserta, paola.daquino@unina2.it

†Department of Mathematics, Seconda Università di Napoli, Via Vivaldi 43, 81100 Caserta, giuseppina.terzo@unina2.it

of a group ring $R[G]$, where R is a unique factorization domain and G is a divisible torsion-free ordered abelian group.

The basic idea introduced originally by Ritt is that of reducing the factorization of an exponential polynomial to that of a classical polynomial in many variables allowing fractional powers of the variables. In general, if we consider an irreducible polynomial $Q(y_1, \dots, y_p)$ over a field it can happen that for some positive integers μ_1, \dots, μ_p the polynomial $Q(y_1^{\mu_1}, \dots, y_p^{\mu_p})$ becomes reducible. This may occur when we work with exponential polynomials. Ritt and Gourin saw the relevance, in terms of factorization, of understanding the ways in which an irreducible polynomial $Q(y_1, \dots, y_p)$ becomes reducible once the variables are replaced with their powers. The determination of the integers μ 's for which the reducibility occurs is a crucial step in their results. More precisely, they give a uniform bound for the number of irreducible factors of $Q(y_1^{\mu_1}, \dots, y_p^{\mu_p})$ which depends only on the degree of $Q(y_1, \dots, y_p)$. van der Poorten in [3] refined the bound by proving that it depends only on the degrees of two of the n variables.

In this paper, we generalize the main ideas due to Ritt to the ring of exponential polynomials in many variables over an algebraically closed field of characteristic 0 with an exponentiation. We produce a theorem of complete reducibility for exponential polynomials with any iterations of exponentiation.

2 E -polynomial ring

Definition 2.1. *An exponential ring, or E -ring, is a pair (R, E) with R a ring (commutative with 1) and*

$$E : (R, +) \rightarrow (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R , satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E -field if K is a field.

We now recall the construction of the ring of exponential polynomials (E -polynomials) over an E -field (K, E) and some of its basic properties. The construction is well known (see [1] or [2]), but for the proof of the main result of this paper we prefer to go through the details. From now on we will be working with (K, E) an algebraically closed field of characteristic 0 with an exponentiation, unless otherwise specified.

The ring of exponential polynomials (E -polynomials) in the indeterminates $\overline{x} = x_1, \dots, x_n$ is an E -ring constructed as follows by recursion. We construct three sequences:

1. $(R_k, +, \cdot)_{k \geq -1}$ are rings;
2. $(B_k, +)_{k \geq 0}$ are torsion free divisible abelian groups;
3. $(E_k)_{k \geq -1}$ are partial E -morphisms.

Step 0: Let

$$R_{-1} = K;$$

$$R_0 = (K[\overline{x}], +, \cdot);$$

$$B_0 = \langle \overline{x} \rangle, \text{ the ideal generated by } \overline{x}. \text{ So } R_0 = R_{-1} \oplus B_0;$$

$E_{-1} : R_{-1} \longrightarrow R_0$, is the composition of the initial E -morphism over K with the immersion of K into $K[\overline{x}]$.

Inductive step:

Suppose $k \geq 0$ and R_{k-1} , R_k , B_k and E_{k-1} have been defined in such a way that R_k as additive group is

$$R_k = R_{k-1} \oplus B_k, \text{ and } E_{k-1} : (R_{k-1}, +) \rightarrow (\mathcal{U}(R_k), \cdot),$$

where $\mathcal{U}(R_k)$ denotes the set of units in R_k .

Let

$$t : (B_k, +) \rightarrow (t^{B_k}, \cdot)$$

be a formal isomorphism. This is used in order to convert an additive group into a multiplicative copy of it. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (as group ring over } R_k\text{)}.$$

Therefore

$$R_k \text{ is a subring of } R_{k+1}$$

and as additive group

$$R_{k+1} = R_k \oplus B_{k+1},$$

where B_{k+1} is the R_k -submodule of R_{k+1} freely generated by t^b , with $b \in B_k$ and $b \neq 0$ (this last condition ensures that B_{k+1} does not coincide with R_{k+1}).

We define

$$E_k : (R_k, +) \rightarrow (\mathcal{U}(R_{k+1}), \cdot)$$

as follows $E_k(q) = E_{k-1}(r) \cdot t^b$, for $q = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

We have constructed a chain of partial E -rings (the domain of exponentiation of R_{k+1} is R_k)

$$R_0 \subset R_1 \subset R_2 \cdots \subset R_k \subset \cdots$$

Then the E -polynomial ring is

$$K[\overline{x}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k$$

and the E -ring morphism defined on $K[\overline{x}]^E$ is defined as follows

$$E(q) = E_k(q), \text{ if } q \in R_k \text{ and } k \in \mathbb{N}.$$

Notice that each R_{k+1} as additive group is the direct sum $K \oplus B_0 \oplus B_1 \oplus \cdots \oplus B_{k+1}$. Moreover, as an additive group $K[\overline{x}]^E$ is

$$K \oplus B_0 \oplus B_1 \oplus \cdots \oplus B_{k+1} \oplus \cdots$$

For all k the group ring R_{k+1} can be viewed in the following different ways

$$R_{k+1} \cong R_0[t^{B_0 \oplus B_1 \oplus \cdots \oplus B_k}];$$

$$R_{k+1} \cong R_1[t^{B_1 \oplus \cdots \oplus B_k}];$$

...

...

$$R_{k+1} \cong R_k[t^{B_k}].$$

Moreover, $K[\overline{x}]^E = R_0[t^{B_0 \oplus B_1 \oplus \cdots \oplus B_k \cdots}]$, i.e. $K[\overline{x}]^E$ is a group ring constructed over a unique factorization domain, $R = K[\overline{x}] (= R_0)$ and a torsion free divisible abelian group $G = t^{B_0 \oplus B_1 \oplus \cdots \oplus B_k \cdots}$ (a \mathbb{Q} -vector space).

If $f \in K[\overline{x}]^E$ then there is a unique k such that $f \in R_{k+1} \cong R_0[t^{B_0 \oplus B_1 \oplus \cdots \oplus B_k}]$ and $f \notin R_k$. In this case f can be written uniquely as

$$f = \sum_{h=1}^N a_h t^{\alpha_h}, \tag{3}$$

where $a_h \in R_0$ and the $\alpha_h \in B_1 \oplus \cdots \oplus B_k$.

Definition 2.2. Let $f \in K[\overline{x}]^E$ be as in (3). The support of f , denoted by $\text{supp}(f)$, is the \mathbb{Q} -vector space generated by $\alpha_1, \dots, \alpha_N$.

Remark 2.3. From the construction $B_1 \oplus \dots \oplus B_k$ is a torsion free abelian group, and using a compactness argument it can be made into an ordered group with order $<$. Without loss of generality, at the cost of the renumbering the α 's we can assume that

$$\alpha_1 < \alpha_2 < \dots < \alpha_N.$$

We recall some properties which are preserved from the E -ring (K, E) to $K[\bar{x}]^E$, the ring of E -polynomials.

Proposition 2.4. *If K is an integral E -domain of characteristic 0 then the E -polynomial ring $K[\bar{x}]^E$ is an integral domain whose units are of the form $uE(\alpha)$, where u is a unit of K , and α is an exponential polynomial.*

Note that if the exponential map is surjective (as over \mathbb{C}) then the units correspond to purely exponential terms.

Definition 2.5. *An exponential polynomial $f \in K[\bar{x}]^E$ is irreducible if there are no non-units g and h with $f = gh$.*

3 Associate polynomial

Using the ideas of Ritt we associate to any exponential polynomial a classical polynomial in many variables over a unique factorization domain. This is a crucial step in order to obtain a factorization theorem for the exponential ring $K[\bar{x}]^E$.

Let $f \in K[\bar{x}]^E$

$$f = \sum_{h=1}^N a_h t^{\alpha_h}, \quad (4)$$

where $a_h \in K[\bar{x}]$ and $\alpha_h \in B_1 \oplus \dots \oplus B_k$. If $\{\mu_1, \dots, \mu_p\}$ is a \mathbb{Q} -basis of $\text{supp}(f)$ then

$$\alpha_h = r_{h1}\mu_1 + \dots + r_{hp}\mu_p$$

for all $h = 1, \dots, N$, and $r_{hj} \in \mathbb{Q}$. Notice that we can always find a new basis for $\text{supp}(f)$ so that r_{hj} 's are integers. Indeed, if M is the least common multiple of the denominators of r_{hj} 's then there are integers s_{i1}, \dots, s_{ip} such that

$$\alpha_h = s_{h1}\frac{\mu_1}{M} + \dots + s_{hp}\frac{\mu_p}{M}$$

for $h = 1, \dots, N$. Let $\nu_1 = \frac{\mu_1}{M}, \dots, \nu_p = \frac{\mu_p}{M}$. Clearly, ν_1, \dots, ν_p is a new basis of $\text{supp}(f)$, and each α_h can be expressed as a linear combination of ν_1, \dots, ν_p with integer coefficients.

Let $y_1 = t^{\nu_1}, \dots, y_p = t^{\nu_p}$. Notice that the linear independence of ν_i 's implies the algebraic independence of $t^{\nu_1}, \dots, t^{\nu_p}$. By expressing each α_i in terms of the ν_j 's we have that f is transformed into a classical Laurent polynomial Q over $K[\bar{x}]$ in the variable y_1, \dots, y_p . This means that we can write Q as a product of a polynomial in the y_i 's and a quotient of a monomial in the y_i 's.

We have the following correspondence:

$$f \in K[\bar{x}]^E \rightsquigarrow Q(y_1, \dots, y_p) \in R[y_1, \dots, y_p]$$

where $R = K[\bar{x}]$. We will refer to $Q(y_1, \dots, y_p)$ as the associate polynomial of f .

Remark 3.1. The correspondence between f and Q holds modulo a monomial in y_1, \dots, y_p , which corresponds to an invertible element of $K[\bar{x}]^E$, and it does not have any consequence on the factorization of f .

Definition 3.2. An exponential polynomial f is simple if $\dim(\text{supp}(f)) = 1$.

An example of a simple polynomial in $\mathbb{C}[x]^E$ is

$$\sin(2\pi x) = \frac{e^{2\pi ix} - e^{-2\pi ix}}{2i}$$

A classical polynomial $Q(y_1, \dots, y_p)$ is *essentially 1-variable* if there are monomials τ_1, τ_2 in y_1, \dots, y_p such that $Q(y_1, \dots, y_p) = \tau_1 P(\tau_2)$, where P is a polynomial in just one variable. Hence, a simple exponential polynomial has associated an essentially 1-variable polynomial. In other words, a simple polynomial is a polynomial in $e^{\mu x}$, where μ is a generator of $\text{supp}(f)$.

An example of an essentially 1-variable polynomial is

$$Q(x, y) = x^2 y (3x^3 y^9 - 2x^2 y^6 + 1) = \tau_1 P(\tau_2),$$

where $\tau_1 = x^2 y$, $\tau_2 = xy^3$ and $P(z) = 3z^3 - 2z^2 + 1$.

3.1 Classical polynomials in many variables

The correspondence between exponential polynomials and classical polynomials implies that there are connections between factorizations of one in terms of factorizations of the other one, and vice versa. Ritt in [7] detected that the classical factorization of a polynomial in many variables could not exhaust all the factorizations of the exponential polynomial, and he introduced factorizations in fractional powers of the variables. In the context of exponential polynomials over an exponential field fractional powers of an exponential do make sense. Refinements of his

ideas where obtained by Gourin in [5], and more recently by van der Porten and Everest in [3] and [4].

Let $Q(y_1, \dots, y_p) \in F[y_1, \dots, y_p]$ be an irreducible polynomial over F , where F is a field or a unique factorization domain. It can happen that for some $\mu_1, \dots, \mu_p \in \mathbb{N} - 0$, $Q(y_1^{\mu_1}, \dots, y_p^{\mu_p})$ becomes reducible. For example, if $Q(x, y) = x - y$ then $Q(x^3, y^6) = (x - y^2)(x^2 + xy^2 + y^4)$.

Definition 3.3. A polynomial $Q(y_1, \dots, y_p)$ is power irreducible (over F) if for each $\mu_1, \dots, \mu_p \in \mathbb{N} - 0$, $Q(y_1^{\mu_1}, \dots, y_p^{\mu_p})$ is irreducible.

Definition 3.4. A polynomial $Q(y_1, \dots, y_p)$ is primary in the variable y_i if

$$Q(y_1, \dots, y_p) = P(y_1, \dots, y_i^d, \dots, y_p)$$

for some polynomial $P(y_1, \dots, y_p) \in K[y_1, \dots, y_p]$ implies $d = 1$. Equivalently, $Q(y_1, \dots, y_p)$ is primary in y_i if the g.c.d. of the exponents of y_i in all terms of Q is 1.

Definition 3.5. A polynomial $Q(y_1, \dots, y_p)$ is primary if it is primary in each variable.

Example 3.6. $Q(x, y) = 3x^2y - 5y^3 + x^3$ is primary in both x and y . On the contrary, $R(x, y) = 3x^2y - 5y^3 + x^4$ is not primary in x since $R(x, y) = P(x^2, y)$, where $P(x, y) = 3xy - 5y^3 + x^2$

Remark 3.7. Notice that if $Q(y_1, \dots, y_p)$ is a non primary polynomial then there exists a unique p -tuple t_1, \dots, t_p of positive integers such that

$$Q(y_1, \dots, y_p) = P(y_1^{t_1}, \dots, y_p^{t_p})$$

where $P(y_1, \dots, y_p)$ is primary. We will see that it is not restrictive to work with primary polynomials in connection to the factorization of an exponential polynomial.

4 Factorization Theorem

In this section we analyze factorizations of f in terms of factorizations of $Q(y_1, \dots, y_p)$ in fractional powers of y_1, \dots, y_p over a unique factorization domain R of characteristic 0 containing all roots of unity.

If fractional powers are permitted then a binomial as $y - 1$ defined over an algebraically closed field K may have infinitely many factors. Indeed, $y^{\frac{1}{k}} - \epsilon$, where ϵ is a k th root of unity, is a factor of $y - 1$ for any positive integer k . So, any general

discussion of factorization in fractional power must avoid such polynomials because of the infinitely many factors they may have.

We recall that a simple polynomial f has associated an essentially 1-variable polynomial $Q(y)$ which factorizes over the algebraic closure R^{alg} of $R(= K[\bar{x}])$ into a finite number of polynomials of the form $1+ay$ with $a \in R^{alg}$. As observed before if fractional powers of the variables are allowed, $1+ay$ has factors of the form $1+a'y^{\frac{1}{k}}$ for $k = 1, 2, 3, \dots$, and $a' \in R^{alg}$. For this reason in the factorization theorem fractional powers of the variable will be avoided for simple polynomials.

4.1 Main result

Ritt and Gourin (1927-1930), and van der Poorten (1995) studied factorizations of $Q(y_1, \dots, y_p)$ into primary irreducible polynomials in the ring generated over an algebraically closed field K of characteristic 0 by all fractional powers of y_1, \dots, y_p . More precisely they proved the following theorem:

Theorem 4.1 ([7],[5]). *There is a uniform bound for the number of primary, irreducible factors of*

$$Q(y_1^{\mu_1}, \dots, y_p^{\mu_p})$$

for $Q(y_1, \dots, y_p)$ not effectively 1-variable, and arbitrary $\mu_1, \dots, \mu_p \in \mathbb{N}_+$. The bound depends only on

$$M = \max\{d_{y_1}, \dots, d_{y_p}\}$$

where d_{y_i} denotes the y_i -degree.

van der Poorten in [3] obtains a bound in terms of the degrees of only two variables.

As a consequence the following corollary holds.

Corollary 4.2. *The number of irreducible factors of $Q(y_1, \dots, y_p)$ in fractional powers of y_1, \dots, y_p is finite.*

The factorization of an exponential polynomial f is obtained via the factorization of the associate polynomial Q in fractional powers of the variables. Indeed, finite factorizations of f generate factorizations of Q in fractional powers of the variables, and vice versa. One implication depends on the following main lemma.

Lemma 4.3. *Let $f(\bar{x}) \in K[\bar{x}]^E$ and suppose that $f(\bar{x}) = g(\bar{x}) \cdot h(\bar{x})$, where $g(\bar{x}), h(\bar{x}) \in K[\bar{x}]^E$. Then $\text{supp}(g), \text{supp}(h)$ are contained in $\text{supp}(f)$.*

Proof: Let $f(\bar{x}) = a_1 t^{\alpha_1} + a_2 t^{\alpha_2} + \dots + a_N t^{\alpha_N}$, and suppose that

$$f = (b_1 t^{\beta_1} + b_2 t^{\beta_2} + \dots + b_M t^{\beta_M}) \cdot (c_1 t^{\gamma_1} + c_2 t^{\gamma_2} + \dots + c_S t^{\gamma_S}), \quad (5)$$

where $g = b_1 t^{\beta_1} + b_2 t^{\beta_2} + \dots + b_M t^{\beta_M}$ and $h = c_1 t^{\gamma_1} + c_2 t^{\gamma_2} + \dots + c_S t^{\gamma_S}$.

Without loss of generality (see Remark 2.3) we can assume

$$\alpha_1 < \alpha_2 < \dots < \alpha_N,$$

$$\beta_1 < \beta_2 < \dots < \beta_M,$$

$$\gamma_1 < \gamma_2 < \dots < \gamma_S.$$

First of all we show that $\text{supp}(h)$ is contained in the \mathbb{Q} -space generated by $\text{supp}(f)$ and $\text{supp}(g)$, i.e. $\text{supp}(h) \subseteq \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. Suppose by contradiction that $\text{supp}(h) \not\subseteq \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. Let γ be the maximum of $\gamma_1, \gamma_2, \dots, \gamma_S$, such that γ is not in $\langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. If there are no β_i in g and γ_j in h such that $\beta_i + \gamma_j = \beta_M + \gamma$, this means that the term $t^{\beta_M + \gamma}$ does not cancel out and $\beta_M + \gamma = \alpha_k$ for some $k = 1, \dots, N$, so $\gamma \in \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. Otherwise, suppose that there are some β_i and γ_j such that $\beta_M + \gamma = \beta_i + \gamma_j$. Since $\beta_M > \beta_i$, then it must be $\gamma_i > \gamma$, and so $\gamma_i \in \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. Hence, $\gamma = -\beta - \beta_i + \gamma_i$ is in $\langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. In both cases we have a contradiction. Hence, $\text{supp}(h) \subseteq \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}}$. We can repeat a similar argument for g , and we obtain that $\text{supp}(g) \subseteq \langle \text{supp}(f), \text{supp}(h) \rangle_{\mathbb{Q}}$. The previous two inclusions, clearly, imply that

$$\langle \text{supp}(f), \text{supp}(h) \rangle_{\mathbb{Q}} = \langle \text{supp}(f), \text{supp}(g) \rangle_{\mathbb{Q}} = \langle \text{supp}(f), \text{supp}(g), \text{supp}(h) \rangle_{\mathbb{Q}}.$$

It remains to prove that

$$\text{supp}(g), \text{supp}(h) \subseteq \text{supp}(f).$$

Suppose by contradiction that it is not. Let d_1, \dots, d_t be a \mathbb{Q} -basis of $\langle \text{supp}(f), \text{supp}(g), \text{supp}(h) \rangle_{\mathbb{Q}}$. We can write β_M, γ_s in terms of this basis and in particular we can write their sum as a \mathbb{Q} -linear combination of d_1, \dots, d_t . The order of the β_i 's and γ_j 's implies that the term $t^{\beta_M + \gamma_S}$ does not cancel out and so, by relation (5), $\beta_M + \gamma_S = \alpha_N$. This contradicts the \mathbb{Q} -linear independence of d_1, \dots, d_t . This completes the proof. \square

Previous lemma implies the following corollary.

Corollary 4.4. *Suppose f factorizes as $f = gh$. Let Q , P and R be the associate polynomials to f , g and h , respectively. There is a monomial τ such that $Q = P'R'$ where $P' = P\tau$, $R' = \tau^{-1}R$.*

Remark 4.5. If f is a simple polynomial and g divides f then g is also simple.

Factorizations of the associate polynomial do not exhaust all the factorizations of f . We need the following crucial result which is a generalization of Theorem 4.1 for polynomials over a unique factorization domain containing all roots of unity. This ensures that the number of irreducible factors in fractional powers of the variables of a polynomial is finite.

Theorem 4.6. *Let $Q(y_1, \dots, y_p)$ be a primary irreducible polynomial over R , a unique factorization domain of characteristic 0 containing all roots of unity. Assume also that Q is not essentially a 1-variable polynomial. Then $Q(y_1, \dots, y_p)$ has a factorization into primary irreducible polynomials in the ring generated over R by all fractional powers of y_1, \dots, y_p , and the number of these irreducible factors is finite.*

We will not give the detailed proof of Theorem 4.6 since it can be obtained step by step following the corresponding proof of the analogue result in [5]. As already remarked the main difference of our results is that we work over a unique factorization domain $R(= K[\overline{x}])$ containing all roots of unity since K is an algebraically closed field while in [5] the polynomials are over \mathbb{C} . In [5] a non essentially 1-variable polynomial corresponds to a polynomial with at least three terms since the polynomials are over \mathbb{C} . In some of our arguments we will tacitly work over the algebraic closure of R , and this is not a restriction with respect to the finiteness of the number of irreducible factors of a polynomial.

First of all notice that any factorization of $Q(y_1^{t_1}, \dots, y_p^{t_p})$ for $t_1, \dots, t_p \in \mathbb{N}$ gives a factorization in fractional powers of the variables of $Q(y_1, \dots, y_p)$. Hence the factorizations of $Q(y_1^{t_1}, \dots, y_p^{t_p})$ are relevant.

The main steps of the proof can be summarized as follows.

Step 1. For $i = 1, \dots, p$ let ϵ_i be a primitive t_i th root of unity, and consider the transformations $\tau_{\epsilon_i} : y_i \mapsto \epsilon_i^k y_i$ for $0 \leq k < t_i$. Let G be the group generated by τ_{ϵ_i} 's, for $i = 1, \dots, p$ and $0 \leq k < t_i$.

The polynomial $Q(y_1^{t_1}, \dots, y_p^{t_p})$ is left unchanged by the action of G on its irreducible factors. This is proved by showing that from one irreducible factor of $Q(y_1^{t_1}, \dots, y_p^{t_p})$ all the others can be obtained via the group G of transformations generated by τ_{ϵ_i} 's.

We recall that Q is an irreducible polynomial and consists of more than two terms, since it is not essentially 1-variable.

Step 2. If the irreducible factor Q_1 of $Q^{(t)}$ is primary then Q_1 also consists of more than two terms.

Step 3. If an irreducible factor Q_1 of $Q^{(t)} = Q(y_1^{t_1}, \dots, y_p^{t_p})$ is primary then each t_j satisfies the relation $t_j \leq M^2$, where $M = \max(d_{y_1}, \dots, d_{y_p})$.

This implies that there are only finitely many sets of positive integers

$$t_{11}, \dots, t_{1p}; t_{21}, \dots, t_{2p}; \dots; t_{n1}, \dots, t_{np}$$

such that $Q(y_1^{t_{i1}}, \dots, y_p^{t_{ip}})$, for $i = 1, \dots, n$ are reducible.

Remark 4.7. The above results have been obtained for Q a primary polynomial. Suppose $Q(y_1, \dots, y_p) = P(y_1^{d_1}, \dots, y_p^{d_p})$ where d_j are positive integers and at least one is strictly greater than 1, and $P(y_1, \dots, y_p)$ is primary. If

$$t_{11}, \dots, t_{1p}; t_{21}, \dots, t_{2p}; \dots; t_{n1}, \dots, t_{np}$$

are the only sets such that $P(y_1^{t_{i1}}, \dots, y_p^{t_{ip}})$, for $i = 1, \dots, n$ are reducible then

$$\tau_{11}, \dots, \tau_{1p}; \tau_{21}, \dots, \tau_{2p}; \dots; \tau_{n1}, \dots, \tau_{np}$$

where $\tau_{ij} = \frac{t_{ij}}{m_{ij}}$ with $m_{ij} = \gcd(t_{ij}, d_j)$, are the only sets of positive integers such that $Q(y_1^{\tau_{i1}}, \dots, y_p^{\tau_{ip}})$, for $i = 1, \dots, n$ are reducible.

We are now in a position to prove the following factorization theorem.

Theorem 4.8. *An element $f \neq 0$ of $K[\bar{x}]^E$, where K is an algebraically closed field of characteristic 0, factors uniquely up to units and associates, as a finite product of irreducibles of $K[\bar{x}]$, a finite product of irreducible of $K[\bar{x}]^E$ whose support is of dimension bigger than 1, and a finite product of elements g_j of $K[\bar{x}]^E$, where $\text{supp}(g_{j_1}) \neq \text{supp}(g_{j_2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.*

Proof: Let $f(\bar{x}) \in K[\bar{x}]^E$, and $Q(y_1, \dots, y_p)$ the associate polynomial. We distinguish between the irreducible factors of Q which are essentially 1-variable polynomials and those which are not. The first ones correspond to the simple factors of f , and we will multiply those which have the same support in order to have all the factors of f of dimension 1 of different support.

Now we consider the irreducible factors of Q which are not essentially 1-variable polynomials, and we study the factorizations of them in fractional powers of the variables. We will show how to get the corresponding irreducible factors of f from them.

Let $P(y_1, \dots, y_p)$ be an irreducible factor of Q not essentially 1-variable. If $P(y_1, \dots, y_p) = V(y_1^{n_1}, \dots, y_p^{n_p})$, for some $n_1, \dots, n_p \in \mathbb{N}$ and $V(y_1, \dots, y_p)$ primary

then necessarily $V(y_1, \dots, y_p)$ is irreducible otherwise $P(y_1, \dots, y_p)$ would be reducible. Once we substitute each y_i by $t^{n_i \nu_i}$ (where ν_1, \dots, ν_p are defined as in Section 3) we get a factor of f . Let r_1, \dots, r_p be positive integers such that

$$V(y_1^{r_1}, \dots, y_p^{r_p}) = V_1 \cdot \dots \cdot V_q$$

where V_j are primary and irreducible, and q is the maximum number of irreducible primary factors. Theorem 4.6 guarantees that such q exists. Indeed, there are only finitely many p -tuples of positive integers n_1, \dots, n_p such that $V(y_1^{n_1}, \dots, y_p^{n_p})$ is reducible. Among these take the one with the highest number of factors which is q .

Claim. The exponential polynomial obtained by replacing y_i by $t^{n_i \nu_i / r_i}$ in V_j for any $j = 1, \dots, q$ is an irreducible factor of f .

Suppose that for some i_0 this is not the case for V_{i_0} . Then for $s_i = mn_i \nu_i / r_i$, where $m = \text{lcm}(r_1, \dots, r_p)$ we have that $V_{i_0}(y_1^{s_1}, \dots, y_p^{s_p})$ is reducible. Hence, $V(y_1^{r_1}, \dots, y_p^{r_p})$ has more than q irreducible factors. We can replace $r_i s_i$ by a submultiple z_i for $i = 1, \dots, p$ in order to have a polynomial $V(y_1^{z_1}, \dots, y_p^{z_p})$ with more than q primary irreducible factors. This is a contradiction with the maximality of q .

We have completed the proof of the existence of a factorization of an exponential polynomial f as a finite product of irreducible not effectively 1-variable polynomials and a finite product of simple polynomials. Now we have to prove that such factorization is unique.

Suppose that $f(\bar{x}) \in K[\bar{x}]^E$ has two different factorizations as

$$f(\bar{x}) = g_1(\bar{x}) \cdot \dots \cdot g_l(\bar{x})$$

$$f(\bar{x}) = h_1(\bar{x}) \cdot \dots \cdot h_s(\bar{x}).$$

It is enough to prove that if $g(\bar{x})$ divides $h(\bar{x}) \cdot l(\bar{x})$ in $K[\bar{x}]^E$ and $g(\bar{x})$ has no factor in common with $h(\bar{x})$ then $g(\bar{x})$ divides $l(\bar{x})$. Suppose

$$g(\bar{x}) \cdot s(\bar{x}) = h(\bar{x}) \cdot l(\bar{x}) \tag{6}$$

for some $s(\bar{x}) \in K[\bar{x}]^E$, and $(g(\bar{x}), h(\bar{x})) = 1$. Let $G(\bar{y}), H(\bar{y}), L(\bar{y}), S(\bar{y})$ be the associate polynomials to $g(\bar{x}), h(\bar{x}), k(\bar{x}), s(\bar{x})$, respectively. Clearly, $(G(\bar{y}), H(\bar{y})) = 1$, since any non trivial common factor of $G(\bar{y})$ and $H(\bar{y})$ would give a non trivial common factor of $g(\bar{x})$ and $h(\bar{x})$.

We saw that any factorization of an exponential polynomial induces a factorization of the corresponding associate polynomial, hence (6) implies the following relation over a unique factorization domain

$$G(\bar{y}) \cdot S(\bar{y}) = H(\bar{y}) \cdot L(\bar{y}). \tag{7}$$

Since G has no common factors with H then G divides L . This implies that the exponential polynomial $g(\overline{x})$ divides $l(\overline{x})$. So the uniqueness of the factorization of f follows. \square

Remark 4.9. The uniqueness of the factorization has the following two important consequences:

1. If f in $K[\overline{x}]^E$ is irreducible and with support of dimension more than 1 then f is prime. For, if f divides gh then by the factorization theorem f must occur in the factorization of one of g or h .
2. In Section 3 in order to construct the associate polynomial to f it was necessary to fix a basis of $\text{supp}(f)$. Clearly, different bases determine different associate polynomials. From the unique factorization of f it follows that they differ by a monomial.

Acknowledgements: The authors would like to thank A. Macintyre for many helpful discussions and insights.

References

- [1] L. van den Dries: *Exponential rings, exponential polynomials and exponential functions*, Pacific Journal of Mathematics, 113, (1), (1984), 51-66.
- [2] A. Macintyre: *Exponential Algebra*, in Logic and Algebra. Proceedings of the international conference dedicated to the memory of Roberto Magari, (A. Ursini et al. eds), Lecture Notes in Pure Applied Mathematics 180, (1991), 191-210.
- [3] A. J. van der Poorten: *Factorisation in fractional powers*, Acta Arithmetica 70, (3), (1995), 287-293.
- [4] A. J. van der Poorten and G. R. Everest: *Factorisation in the ring of exponential polynomials*, Proceedings of the American Mathematical Society, 125, (5), (1997), 1293-1298.
- [5] E. Gourin: *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Transactions of the American Mathematical Society 32, (1930), 485-501.
- [6] L. A. MacColl: *A factorization theory for polynomials in x and in functions $e^{\alpha x}$* , Bulletin American Mathematical Society, (41), (1935), 104-109.

- [7] J.F. Ritt: *A factorization theorem of functions $\sum_{i=1}^n a_i e^{\alpha_i z}$* , Transactions of American Mathematical Society 29, (1927), 584-596.